ELK Guide

Winston Library Installation and Logger Creation

- Install Winston library in your node app using the command:
  - *npm install --save winston*
- The purpose of installing Winston library is that you have to make your logger like I created which can be located in **util** folder named ***logger.js***
- Please check the following links for a detailed description of anything regarding the winston library.
  - https://www.npmjs.com/package/winston
  - https://github.com/winstonjs/winston
- Tutorial’s link:
  - https://www.youtube.com/watch?v=cWi7TAyVoZo&t=741s&ab_channel=ProgrammingwithBasar

ELK Setup and How to Use It

- Please watch these two links for ELK setup and how to pass and visualize data using it:
  - *https://www.youtube.com/watch?v=8iXZTS7f_hY&ab_channel=ProgrammingKnowledge*
  - *https://www.youtube.com/watch?v=_kqunm8w7GI&ab_channel=ProgrammingKnowledge*
- **Note:**
  - *At this point, elk must be added to your environment variables to run the below commands.*
  - *It doesn’t matter whether you run your cmd with admin rights or not, it works.*
- To check if your ***logstash.conf*** file is correct or not, use this command:
  - *logstash -f <absolute-path-of-your-conf-file> --config.test_and_exit*
- To autorun your ***logstash.conf*** file on edit, use this command:
  - *logstash -f <absolute-path-of-your-conf-file> --config.reload.automatic*

- Find all logstash commands here:
  - https://www.elastic.co/guide/en/logstash/current/running-logstash-command-line.html#running-logstash-command-line

Access Index and Visual Logs using Kibana

- Once you have successfully passed your data to elasticsearch using logstash, you can access your index (custom name to uniquely identify logs on Kibana).
- On Kibana server, access these from the menu;
  - To create an index pattern:
    - *(Management)Stack Management>(Kibana)Index Patterns*
  - To view your logs:
    - *(Management)Dev Tools*
    - **Command:** *GET /<your index>/_search*
  - To view specific fields or search within logs:
    - *(Analytics)Discover*
    - Update date and time from top-left side and **DON'T** forget to click on the update button at this moment. You need to update each time you change the date and time.
    - Select fields from available fields by clicking on the **+** icon next to each field
    - Search some text in the search bar and update again.
  - To create any kind of graph/chart/table of your logs:
    - *(Analytics)Visualize Library>Aggregation based*
    - And, select your desired graph/chart/table and visualize your logs

Congratulations, you have successfully learned ELK basics!!!

Good Luck!